

United States Patent Application

Of

Marc David Abrahams
Seda Gragossian

**A SYSTEM FOR UBIQUITOUS NETWORK PRESENCE AND
ACCESS WITHOUT COOKIES**

Express Mail Mailing Label No.
EV 333 464 305 US

**A SYSTEM FOR UBIQUITOUS NETWORK PRESENCE AND ACCESS
WITHOUT COOKIES**

5

BACKGROUND OF THE INVENTION

The present invention relates generally to computer network access, and more particularly to ubiquitous network presence.

As the variety of devices capable of Internet access continues to grow so do the number of such devices that do not run conventional World Wide Web (Web) browsers, or any browser at all. This causes a more difficult problem in providing methods for ubiquitous login to users of such devices. Currently, most methods utilize setting cookies in the Web browser of the device. These cookies (files that are stored on a user's computer by a web site and that can identify a return visit) are automatically sent to servers the user encounters giving the single login effect. If the device cannot manage cookie methods of identification, they cannot have the single login effect.

There is thus a need in the art for a system for ubiquitous network presence that does not require utilization of cookies for devices that cannot manage cookie methods of identification.

SUMMARY OF THE INVENTION

The present invention advantageously addresses the needs above as well as other needs by providing a system for ubiquitous network presence that does not require utilization of cookies for devices that cannot manage cookie

methods of identification.

In one embodiment, the invention can be characterized as a method for computer network access comprising the steps of communicating user information to a first server from a client, storing user information on the first server, creating a unique identification for the user, storing the unique identification on the first server, communicating the unique identification to the client and other servers, storing the unique identification on the client and other servers, and matching the unique identification stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers.

In another embodiment, the invention can be characterized as a computer network system comprising a server computer running a server software application operable for creating a unique identification for a user, storing the unique identification on the server computer, communicating the unique identification to a client and authenticating the user via the unique identification when the user communicates with the server computer. The system also comprises a client computer running a client software application, said client computer operably connected to the server computer over a network and wherein the client software application is operable for communicating user information to the server application software from the client computer, storing user information on the client computer, and performing the user authentication with the server application.

A better understanding of the features and advantages of the present invention will be obtained by reference to the following detailed description of the

invention and accompanying drawings which set forth an illustrative embodiment in which the principles of the invention are utilized.

5

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other aspects, features and advantages of the present invention will be more apparent from the following more particular description thereof, presented in conjunction with the following drawings wherein:

FIG. 1 is a diagram of the system architecture of a network according to an embodiment of the present invention.

15 FIG. 2 is a chart displaying a process according to an embodiment of the present invention.

Corresponding reference characters indicate corresponding components throughout the several views of the drawings.

20

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following description of the presently contemplated best mode of practicing the invention is not to be taken in a limiting sense, but is made merely for the purpose of describing the general principles of the invention. The scope of the invention should be determined with reference to the claims.

30 Referring to FIG. 1, shown is a diagram of the system architecture of a network according to an embodiment of the present invention.

Shown is a customer device 100, the Internet 105, firewalls 110, a business network communication link 112, a registration server 115, a back-end server 120, a billing database server 125, a public switched telephone network (PSTN) Gateway database 130, and other database servers 135.

The customer device 100 is connected through the Internet 105 to the front end registration server 115 (preferably through a firewall 110). The customer device may include any electronic device that has digital communications capability such as a computer, cell phone, personal digital assistant or television, for example. The front end registration server 115 is linked to a business network including the back-end server 120, the billing database server 125, the PSTN Gateway database 130 and other database servers 135 through the business network communication link 112. Each node in the business network preferably requires access through network firewall protection 110.

A client side application runs on the customer device 100 and functions to control an amount of set up data stored on any customer device 100. The client application, instead of a web browser, provides a connection to networked services available on the business network. This client application runs on the customer device 100 in the background to perform authentication with the services the customer accesses through the database servers 125, 130, 135 with the customer device 100.

When a customer initially registers with a web site they enter their customer information such as their address and phone number, for example. This can be done via any variety of input devices such as a keyboard, mouse, remote control, touchscreen or voice recognition technology

to name a few. The back end server 120 accepts that information 210 via common gateway interface (CGI) standard. CGI is a standard for interfacing external applications with information servers, such as Hypertext Transfer Protocol
5 (HTTP) or World Wide Web servers. Here, the external application is that running on the customer device 100 and the information server is the back end server 120. Berkeley System Distribution (BSD) socket interface (socket), JAVA servlet technology (servlet) or other suitable interfaces
10 may also be used. The customer's information is then stored on the back end server 120 in a database. The server application running on the back end server 120 then creates a unique customer ID for the customer by using a random number generator, for example, and stores it in the
15 database. This unique customer ID is communicated via the Internet from the server application to the client application on the customer device 100 and preferably stored in non-volatile memory on the customer device 100.

The server application also communicates this
20 customer ID and any other necessary customer information 230 via the business network to all server applications of services that are provided by the business network including those running on the other servers 125, 130, 135 on the business network. This network communication may be done
25 through a variety of means such as CGI, servlet or socket, for example, and may be formatted in Extensible Markup Language (XML), custom format, or other suitable means. The server application for the particular service the customer is attempting to access then authenticates the user via the
30 unique customer ID by matching the unique customer ID communicated by the client application to the server application with that unique ID stored on the server's

database (say server 125 for example in FIG. 1). The user is then logged on to access the requested services.

When the customer subsequently attempts to access services on the business network the customer will have a unique ID that was created during the initial log on, and again the server application for the particular service the customer is attempting to access will automatically authenticate the user via the unique customer ID from the client by matching it with that unique ID stored on the server's database. This provides ubiquitous presence on the business network for the customer for whatever services they desire to access without the use of cookies.

Referring next to FIG. 2, shown is a chart displaying a process according to an embodiment of the present invention.

When a customer initially registers with a web site they do not have a unique customer ID 200 and they enter their customer information 205 such as their address and phone number, for example. This can be done via any variety of input devices such as a keyboard, mouse, remote control, touchscreen or voice recognition technology to name a few. The back end server 120 accepts that information 210 via common gateway interface (CGI) standard. CGI is a standard for interfacing external applications with information servers, such as Hypertext Transfer Protocol (HTTP) or World Wide Web servers. Here, the external application is that running on the customer device 100 and the information server is the back end server 120. Berkeley System Distribution (BSD) socket interface (socket), JAVA servlet technology (servlet) or other suitable interfaces may also be used. The customer's information is then stored 215 on the back end server 120 in a database. The server

application running on the back end server 120 then creates a unique customer ID 220 for the customer by using a random number generator, for example, and stores it in the database. This unique customer ID is communicated via the Internet from the server application to the client application on the customer device 100 and preferably stored in non-volatile memory on the customer device 100. The server application also communicates this customer ID and any other necessary customer information 230 via the business network to all server applications of services that are provided by the business network including those running on the other servers 125, 130, 135 on the business network. This network communication may be done through a variety of means such as CGI, servlet or socket, for example, and may be formatted in Extensible Markup Language (XML), custom format, or other suitable means. The server application for the particular service the customer is attempting to access then authenticates 235 the user via the unique customer ID by matching the unique customer ID communicated 240 by the client application to the server application with that unique ID stored on the server's database (say server 125 for example in FIG. 1). The user is then logged on 245 to access the requested services.

When the customer subsequently attempts to access services on the business network the customer will have a unique ID 200 that was created during the initial log on, and again the server application for the particular service the customer is attempting to access will automatically authenticate 235 the user via the unique customer ID from the client 240 by matching it with that unique ID stored on the server's database. This provides ubiquitous presence on the business network for the customer for whatever services

they desire to access without the use of cookies. This process may be useful for automatically tracking customer usage of services without requiring interaction from the customer such as for billing, customer locating, customer preferences and other purposes.

While the invention herein disclosed has been described by means of specific embodiments and applications thereof, numerous modifications and variations could be made thereto by those skilled in the art without departing from the scope of the invention set forth in the claims.

15

20

25

30